BUILDING TRUST AND CONFIDENCE IN ELECTRONIC COMMERCE:

A Framework for Electronic Authentication in Canada

Prepared by the Electronic Commerce Branch
Industry Canada
July 2000

This document and related materials are available electronically on the World Wide Web at the following address: **(http://e-com.ic.gc.ca/)**.

Aussi disponible en français sous le titre *Instaurer la confiance à l'égard du commerce électroniue : Cadre pour l'authentification électronique au Canada*

100-06792/

About this Document

This paper has been prepared by Industry Canada's Electronic Commerce Branch (formerly the Electronic Commerce Task Force) as part of ongoing work in support of Canada's leadership in electronic commerce. It relates to that part of Canada's electronic commerce strategy that has identified the need to build trust and confidence in the global digital economy. The paper forms part of the consultation program currently underway with key stakeholders[1] to discuss how authentication and certification services could develop in Canada.

In October 1998, the Government of Canada announced its cryptography policy including the determination that it would not regulate private sector entities providing authentication and certification services. The Electronic Commerce Branch subsequently embarked on a consultation program to discuss with stakeholders how private sector authentication and certification services could develop in Canada and to determine if barriers exist to investment or use.

The elements of the consultation program that have been completed to date include a series of bilateral discussions. This preliminary round of consultations indicated that there is a need for ongoing public/private sector dialogue in this area and that many of the issues need to be addressed on a collaborative basis.

Following on these bilateral consultations, a workshop was held in December 1999 that brought together a broader group of stakeholders to extend the collective understanding of the opportunities and challenges inherent in developing and rolling out these services in Canada and to identify initiatives that the private and public sectors could undertake to exploit the opportunities and address the challenges. Stakeholders agreed that the views of a wider audience should be considered and that a consultation paper that proposes a framework should be developed for progressing this work.

This paper describes electronic authentication and certification services and provides some background on the existing policy framework. It identifies the need to provide a co-ordinated approach that a framework be established for these services and that international dimensions must be taken into consideration.

Industry Canada's approach has been to use high-level parameters to define authentication and certification services given that the federal government's interests lie predominantly in broad policy aspects of authentication services. Further, Industry Canada recognizes that different applications will require different solutions and, therefore, has endeavoured to take a

---

[1] Stakeholders include representatives of the private sector, consumer groups and some provinces. See ***Appendix A*** for a complete list. For more information on the various elements of the consultation program see **(http://e-com.ic.gc.ca/english/authen/631e10.html)**.

technology and architecturally neutral approach. It has not focussed on any specific security solution.

However, aspects of this paper focus on the issues associated with digital signatures in view of the predominant role played by public key cryptography in this emerging environment. Future work will address issues associated with technical alternatives to public key cryptography as they are developed.

This paper reflects the findings of the Branch's consultative processes. It also has benefited from input from the Office of Consumer Affairs and the Bureau of Competition Policy and from the Treasury Board Secretariat. The proposals it contains raises important questions regarding the development and use of authentication and certification services in Canada on which Industry Canada seeks broader stakeholder views.

Ongoing public/private sector dialogue has been identified by stakeholders as being essential to advancing the trust agenda in Canada. As the next step in this dialogue, stakeholder groups are encouraged to provide responses to any or all of the questions that appear in the various sections of this paper. ***Appendix C*** has been developed to provide a single point of reference for the questions upon which views and input is sought. Input is also sought on the summary of potential roles in ***Appendix D***.

It is recognized that, as this paper encompasses a wide range of issues and topics, stakeholders may elect to respond only to those questions that relate to their respective areas of interest.

For information about the contents of this paper, the consultation process, or to submit comments on the paper, please contact:

Peter Ferguson
Director, Electronic Commerce Policy
Electronic Commerce Branch
Industry Canada
20th Floor, 300 Slater Street
Ottawa ON K1A 0C8
E-mail: **authen@ic.gc.ca**
Fax: (613) 941-0178

Comments should be sent on or before **September 21, 2000.**

Your comments on the proposed approach discussed in this paper and other related matters are an essential part of a useful dialogue on this subject.

TABLE OF CONTENTS

Introduction and Scope 1
- a) Background 1
- b) Canada's Electronic Commerce Strategy and Agenda 1
- c) Cryptography 2
- d) Authentication and Certification Services Defined 3

Part 1 - Context 5
- 1.1 Existing Policy Framework for Confidence and Trust 5
  - a) Consumer Protection 5
  - b) Privacy 5
  - c) Legal Framework 6
  - d) Security 7

Part 2 - Defining the Forward Agenda 8
- 2.1 Stakeholder Findings 8
  - a) Need for a Framework 8
  - b) Domestic Compatibility 8
  - c) International Compatibility 9
  - d) Competition Dimensions 11
  - e) Market Development Aspects 12
- 2.2 Proposed Scope of Framework 12

Part 3 - Authentication & Certification Services - Proposed Approach 14
- 3.1 General 14
- 3.2 Principles ..... .14
  - a) General 14
  - b) Applicability and Scope 15
  - c) Content 16
  - d) Adherence 18
  - e) Role of public sector CAs (in particular the GOC-PKI) 19
  - f) Mechanism for Developing Principles 19
- 3.3 Principles as a Basis for Accreditation 20

Part 4 - Market Development: Opportunities and Challenges 22
- 4.1 Promoting the Adoption and Use 22
  - a) Position as a strategic investment 22
  - b) Raising consumer awareness and use 23
  - c) Encouraging competition and fostering innovation 25

Part 5: Conclusions and Next Steps 28
5.1 Proposed Next Steps 28

Authentication Consultation Program: Stakeholder Participants ..... Appendix A

Proposed Framework for Discussion of Accreditation Model(s) ..... Appendix B

Summary List of Questions ..... Appendix C

Summary of Potential Public/Private Sector Roles ..... Appendix D

List of Abbreviations

List of Sources

Introduction and Scope

a) Background

Until recently, most on-line transactions were conducted within a private domain or closed community where trading partners and clients are known to one another. The existence of contractual privity of participants in these models has meant that the relationships between the parties are relatively well understood and have a predictable framework for analysis. This is not the case in public domain, open environments (such as the Internet), where parties are strangers and do not have direct trading agreements or contracts. Intermediaries may also be involved. The complex sets of relationships that can potentially be involved raise new and different issues. There is a need to look at solutions that can address the trust and confidence agenda where parties without existing relationships are communicating and transacting.

Cryptography is important to building trust and confidence in electronic markets as it functions to allow parties who do not know each other to exchange and authenticate information and conduct business in a secure manner in an on-line environment. The cryptography-related services involving authentication and certification mechanisms that provide for this functionality are an integral part of addressing the trust agenda in broad-scale electronic commerce.

A wide variety of technologies and mechanisms are available to authenticate and certify electronic transactions and a number of different architectural models exist to administer them. Different kinds of transactions require different kinds of solutions and the choice of technology is driven by the requirements of the applications and the parties involved. New solutions and approaches are emerging daily. On this basis, the evolving market associated with these services is dynamic and diverse.

It is the conclusion of stakeholder consultations to date that competition and innovation will play an important role in this particular market. However, the need to build trust and confidence in authentication and certification services is as important as the need to promote competion and foster innovation.

b) Canada's Electronic Commerce Strategy and Agenda

In September 1998, the Prime Minister announced the *Canadian Electronic Commerce Strategy*[2] and presented a vision for Canada's future in electronic commerce. The framework identifies a number of priorities for action including building trust in the digital economy.

---

[2] For information on the various initiatives that are part of this Strategy see **(http://e-com.ic.gc.ca/english/60.html)**.

While Canada's *Connecting Canadians*[3] agenda's goal is to ensure that Canada is among the leaders in global connectivity[4], access only provides the means to participate in the global electronic commerce marketplace. The Government recognizes that this will translate into real opportunities only if we are also able to fulfill the necessary condition of ensuring trust and confidence in the electronic marketplace.

The October 1999 Speech from the Throne articulates the Government's intention to "take steps to make Canada a centre of excellence in electronic commerce and encourage its use throughout the economy." More recently, in a report prepared by the Canadian E-Business Opportunities Roundtable[5], the leadership position Canada has achieved nationally and internationally has been acknowledged. However, the report also cites the need to rise to the challenge of capitalizing on the full e-business opportunities that are available or risk falling behind other advanced economies. Building trust and confidence in the digital economy is crucial to capitalizing on this opportunity.

c) Cryptography

Cryptography techniques can provide a foundation for establishing the necessary trust in electronic commerce because they ***safeguard*** information, ***protect*** communications and ***authenticate*** parties to transactions. Specifically, they can be used to develop ***digital signatures***[6] that provide for:

i) ***authentication*** - proof that users are who they claim to be (or that computer devices, software, etc. are what they purport to be);

ii) ***integrity*** - so that data cannot be modified without detection; and

---

[3] *Connecting Canadians* is the federal government's vision and plan to make Canada one of the most connected countries in the world. Electronic commerce s a key element of the agenda. See **(http://connect.gc.ca/en/100-e.htm)**.

[4] The Conference Board of Canada "Connectedness rankings" placed Canada second to the United States in overall connectedness (based on a composite index using primarily 1997-98 data). To put this ranking in perspective, current data suggests that over 50% of Canadians are on-line.

[5] *FAST FORWARD: Accelerating Canada's Leadership in the Internet Economy*. The E-Business Roundtable was established by the Boston Consulting Group with the assistance of Industry Canada in June 1999. **(http://e-com.ic.gc.ca/eteam/)**

[6] An electronic identifier attached to an electronic document. Analogous to a handwritten signature. The term is almost always taken to mean an identifier generated by using public key cryptography (see next section). The term *electronic signature* is used in a broader context to indicate processes that include digital signatures.

iii) ***non-repudiation*** - proof that a transaction occurred, or that a message was sent or received (so that parties cannot deny that the exchange occurred).

Cryptographic techniques can also provide for ***confidentiality*** by applying encryption/decryption technologies to mathematically scrambling the original text. This protects information from unauthorized disclosure or viewing.

Thus, cryptography is important to building trust and confidence in electronic markets as it functions to allow parties who do not know each other to exchange and authenticate information and conduct business in a secure manner in an on-line environment. The cryptography-related services involving authentication and certification mechanisms that provide for this functionality are an integral part of addressing the trust agenda.

d) Authentication and Certification Services Defined

While authentication processes have been in use for years in an electronic environment (passwords, personal identification numbers or "PINs", etc.), the techniques used have been largely suitable only for the authentication of entities, not for authenticating data or attributes. Further, these forms of authentication do not, in actual fact, confirm the identity of the entity being authenticated, but rather only that the entity participating in the transaction has the knowledge of the PIN, password or personal information (and where applicable, is in possession of the bank card or other token). Exchanging information and conducting business electronically over various types of open networks gives rise to a need for methods of electronic authentication and a range of related services to support their use.

Electronic authentication can be understood to encompass any method of verifying some piece of information in an electronic environment, whether it is the identity of a sender of a message (or author of a text), the authority of a person to enter into a particular kind of transaction, the security attributes of a hardware of software device, etc. Cryptographic techniques perform this function by using ***digital keys*** [7] to encrypt and decrypt digital data.

There are two major cryptographic methods. In ***secret key cryptography***, the same key is used to encrypt and decrypt the data. In ***public key cryptography***, there are two different, but related keys, and what is encrypted with one can only be decrypted with the other.[8] In addition to the capability to encrypt for confidentiality, public key cryptography enables key holders to make their documents capable of subsequent authentication by using their private

---

[7] A unique combination of ones and zeros.

[8] One key, known as the *public key*, is published in, what might be considered, the equivalent of a telephone book. Its related *private key* is kept secret.

key to create a ***digital signature.***[9] This technique also ensures the integrity of documents and enables recipients to determine if a message has been altered in any way during transmission. It is this functionality that is of particular interest for secure electronic commerce across open networks such as the Internet.

The trustworthy distribution of public keys, combined with procedures to ensure that a specific key genuinely belongs to a particular user, is essential to the use of public key cryptography in open networks. One of the ways this can be accomplished is through the use of a trusted third party (or a ***certification authority - "CA"*** [10]) to manage the distribution of the public keys, and the ***certificates***[11] containing such keys. In addition to containing the key holder's public key, certificates typically contain information data about the certificate itself, the entity to whom the certificate has been issued and data about the certificate issuer. The data is bound to the entity, usually by being digitally signed by the CA.

Certificates may be issued for a number of purposes ranging from providing assurance of identity to providing more detailed information about the certificate holder in order to authorize certain actions, such as conducting transactions. Certificates may also be issued with different levels of assurance that indicate the degree of reliance that can be placed on a certificate.

In order for a certificate to be trustworthy, it must be issued by a credible CA and considerable public policy focus around the world is now concentrating on devising ways to ensure that a CA, and the certificates it issues, are trustworthy. Global electronic commerce has resulted in the need for standard approaches to recognize the level of trustworthiness of digital signatures, proof of identity in cyberspace and mutual trust about the level of trustworthiness of certification authorities across different jurisdictions.

---

[9] An identifier that is attached to, or logically associated with, an electronic message or document. The sender "signs" a message with the private key. The term "digital signature" is almost always taken to mean an electronic signature that is generated using public key cryptography.

[10] For the purposes of this paper, the term *certification authority (CA)* is used to connote a trusted third party although it is recognized that a trusted third party may take alternate forms.

[11] An electronic form similar to an electronic version of a driver's license or passport.

Part 1 - Context

1.1 Existing Policy Framework for Trust and Confidence

In 1996, in response to recommendations from the Information Highway Advisory Council, the Minister of Industry released a comprehensive report on behalf of the Federal Government that detailed the steps to be taken to create a knowledge-based society.[12] With respect to electronic commerce, the report noted the need for secure electronic transactions.

Working in close collaboration with the private sector, the Federal Government has addressed this need specifically, and the related requirement to build trust and confidence in electronic commerce generally, with a variety of policy initiatives in the following areas:

a) Consumer Protection

Industry, government and consumer representatives have jointly developed a set of principles for the protection of consumers conducting transactions online.[13] The principles are intended to guide the actions of businesses, consumers and governments within Canada in the development of a consumer protection framework for electronic commerce over open networks, including the Internet. The principles recognize that a sound framework for consumer protection will promote consumer confidence and facilitate the acceptance and growth of electronic commerce. The Office of Consumer Affairs in Industry Canada is currently working with the private sector and its provincial counterparts to "operationalize" these principles.

b) Privacy

The *Personal Information Protection and Electronic Documents Act* was passed by parliament in April 2000.[14] The provisions in Part 1 of the *Act* establish rules to govern the collection, use and disclosure of personal information and come into force, on January 1, 2001. These privacy provisions will help to build trust in electronic commerce by providing assurances of protection for personal information in digital form. They create a level playing field for business with clear, predictable rules for all. Consumers and

---

[12] *Building the Information Society: Moving Canada into the 21st Century* (May 1996).

[13] *Principles of Consumer Protection for Electronic Commerce: A Canadian Framework* (November 1999). Developed by the Working Group on Electronic Commerce and Consumers (co-ordinated by the Office of Consumer Affairs of Industry Canada). See **http://strategis.ic.gc.ca/SSG/ca01180e.html** for a list of the principles and more information on this work.

[14] Formerly "Bill C-6". For additional information see **(http://e-com.ic.gc.ca/english/privacy/632d1.html)**.

business will be able to conduct their on-line transactions with the confidence that privacy protection measures are in place and that they will be overseen by the Privacy Commissioner.

c) Legal Framework

The new *Personal Information Protection and Electronic Documents Act* also creates an electronic alternative for doing business with the federal government.[15] The relevant provisions, which correspond to Parts 2-4 of the *Act*, pertain to:

i) Secure Electronic Signature:

The *Act* has established that federal departments, agencies and boards will have the authority to decide how requirements in existing statutes and regulations can be satisfied by electronic means. These provisions came into force on May 1, 2000. A key component of the legislation is the concept of a ***secure electronic signature***[16] which may be used in electronic transmissions.

ii) Government On-line:

The new legislation provides a way for the federal government to conduct business through electronic means. What is possible on paper will be possible electronically. The *Act* makes electronic alternatives the equivalent of the paper way of doing things.

iii) Electronic Evidence:

The new legislation clarifies how the courts assess the reliability of an electronic document that is introduced as evidence, authorize regulations to assist the courts in associating secure electronic signatures with persons, and recognizes that notices and acts published electronically by the Queen's Printer have the same legal weight as those published on paper by the Queen's Printer.

---

[15] For more information on these provisions of the *Act* see **(http://e-com.ic.gc.ca/english/fastfacts/43d9.html)** and**(http://canada.justice.gc.ca/en/ps/ec/index.html)**.

[16] Defined as an "electronic signature that results from the application of a technology or process prescribed by regulations ...". These regulations are being developed by the Treasury Board.

d) Security

In October 1998, the Federal Government issued its policy on cryptography that included provisions that relate to its use in the conduct of electronic commerce.[17] The policy responds to the need for certain categories of electronic transactions to be secure by ensuring that Canadians can develop, import and use whatever cryptography products they wish. It contemplates situations where cryptographic techniques provide ways to establish the identity and privileges of the transacting parties, often through the use of trusted third parties, such as certification authorities (CAs). The policy rejects the idea of mandatory licensing of certification authorities and instead, encourages and supports industry-led accreditation of private-sector certification authorities.

---

[17] See **http://e-com.ic.gc.ca/english/crypto/631d1.html** for more information on the cryptography policy.

Part 2 - Defining the Forward Agenda

2.1 Stakeholder Findings

a) Need for a Framework

While stakeholders are of the view that competition and innovation are important objectives in this emerging marketplace, they also acknowledge that new markets develop best when users are confident about the products and services they receive. Stakeholders recognize that the need to build trust and confidence is as important as the need to promote competition. This presents a challenge in terms of arriving at an appropriate and effective balance of interests that meets the needs of all interested parties whether they are suppliers, users or other stakeholders.

The majority of stakeholders have also noted that there are market efficiency costs and questions about public confidence associated with a laissez-faire approach to this new marketplace. They are concerned that the costs and risks are great for all parties as new business processes are developed and implemented. Some stakeholders feel that trust and confidence need to be viewed as a public good that cannot be ensured by market forces alone.

Four reasons have emerged from consultations to date why it is desirable to establish a framework for authentication and certification services.

- to provide a means for users to establish the trustworthiness of certification authorities;
- to establish a consistent and auditable level of trust of authentication schemes;
- to allow for users to make choices based on some known parameters for trust and confidence; and,
- to minimize situations where businesses and consumers, involved in more than one authentication scheme, may be faced with differing (and potentially even conflicting) requirements.

b) Domestic Compatibility

Stakeholders have also pointed out that a framework for authentication and certification services will facilitate sound and consistent legal and technical practices among certification authorities in Canada. Some degree of commonality will also provide for the

compatibility of approaches between industry sectors that is likely to be expected by users at the domestic level.[18]

They have also emphasized that there is also a need for compatibility of approaches across the provinces to avoid barriers and provide for the interoperation that is necessary for national electronic commerce. Stakeholders are of the view that federal and provincial co-ordination is necessary and desirable to achieving this and have suggested that existing fora can be used for this purpose. With respect to the public sector, the Public Sector CIO Council[19] has been identified as a potentially effective means of co-ordination. In terms of public/private sector fora, the Uniform Law Conference of Canada (ULCC)[20] has similarly been identified. The ULCC has already developed the *Uniform Electronic Commerce Act*[21] which is an important initiative aimed at providing a foundation for the co-ordination of provincial legal frameworks.

c) International Compatibility

From an international perspective, a framework can greatly assist in facilitating the recognition of Canadian certificates internationally. International compatibility is important from two perspectives. First, it is important that there is global acceptance and use of Canadian services. Second, there is a need to ensure that Canada meets its international trade obligations. Any failure to meet international norms could restrict Canada's trade with other countries and result in transborder blockages.

The approaches being taken by various jurisdictions are diverse. Thus, the development of a framework that will facilitate recognition of Canadian certificates will not be without its challenges. It is important to take steps to ensure certificates issued by Canadian organizations are accepted by jurisdictions that administer a range of different regimes, from regulated or licensed CAs, to CAs in non-regulated regimes. From a Canadian perspective, where there are to be no federal licensing requirements, the challenges of developing a Canadian approach for international

---

[18] The degree and extent of the compatibility or interoperability that is required or desirable will vary. For instance, its scope could be within industry sectors, across a range of industry sectors or simply up and down the supply chain.

[19] The "PSCIOC" is comprised of Canada's Chief Information Officers (CIOs) from the provinces, territories and the federal government. (**http://www.tbs-sct.gc.ca/cio-dpi/psciоc**)

[20] An independent organization made up of representatives from the bench, governmental law departments and the practicing profession.

[21] September 1999. See (**http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm**).

discussions are likely easier to address where CAs are either uncontrolled or where an industry-led accreditation approach can be adopted promptly.[22] Those jurisdictions where CA services are regulated are likely to present more significant challenges, particularly where cross-border recognition (or cross-certification) is sought. There would appear to be no barriers of this nature operating within the North American environment at this time. However, it is already apparent that there is the potential for barriers to exist in Europe and Asia, and that there is a need to investigate ways of addressing them.[23]

Canada's continued involvement in various international fora to address the need for global frameworks for authentication is, therefore, a critical ongoing dimension to this work. The current focus of Canada's international work in this area is on the United Nations International Commission on International Trade Law (UNCITRAL) for legal discussions, and in the Organization for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) forum for public policy discussions.[24] It is understood that close collaboration between the federal government and the private sector is central to this participation. There are also suggestions from stakeholders that Canada should complement this participation with bilateral or multilateral consultations aimed at

---

[22] Announced by the Minister of Industry in October 1998 in the context of the Cryptography Policy. However, while the Federal Government has indicated it will not pursue licensing approach, the provinces have not as yet done likewise. As such, it is theoretically possible for Canada to end up with a mix of licensed and unlicensed Cas if one or more provincial governments decided to introduce licensing conditions for CAs within their jurisdiction.

[23] It may be difficult for foreign CAs to meet the requirements of either the German or the Italian law and this is the subject of ongoing discussion in international fora. A project that may be particularly useful in identifying potential obstacles to cross-border authentication, is a current initiative of an expert task group of the APEC Telecommunications Working Group. The project involves identifying the key processes for establishing trust in certification processes and mapping existing schemes against these key elements. This work will facilitate a pulling together of the different approaches and provide for an analysis of how the variances might be adapted to meet the same objectives.

[24] The Department of Justice has responsibility for developing Canadian positions for the work within UNCITRAL. Electronic Commerce Branch representatives participate in the relevant OECD/APEC committees and working groups.

developing memorandums of understanding or joint statements with additional countries and jurisdictions.[25]

The discussion of compatibility at the international level points to the important continuing role of governments as "trust leaders" in this environment. The need for businesses to develop trust relationships internationally suggests that governments will continue to play an important role since the current array of private sector initiatives aimed at developing global frameworks may require some form of government support, especially those of a cross-sectoral basis. Many of these private sector-led initiatives (for example, the relevant committees under the American Bar Association, the new PKI Forum,[26] etc.) already provide for participation by government representatives.

d) Competition Dimensions

Stakeholders have observed that the authentication and certification services marketplace is nascent with few suppliers and limited competition. It has also been observed that the market offers new opportunities for some business sectors giving players, not previously involved in certain aspects of electronic commerce, the technology to offer new services and assume new roles. Stakeholders have expressed concern that market solutions alone will not necessarily lead to a level playing field for all players. For example, it has been pointed out that, there may not be a level playing field where regulated entities are competing against entities that do not fall under any regulatory supervision. An uneven playing field could have implications for end users since the level of protection afforded to users may differ. If users are unable to differentiate among CAs due to the complexity of the technology and services provided, there is the potential for confusion, hidden costs, and greater (unknown) risk with resulting frustration and confusion. The introduction of a framework for authentication in Canada can assist in levelling the playing field for all players.

---

[25] Currently, Canada has joint statements with Australia and the European Union. While they apply to electronic commerce generally, it is possible that additional consultations and negotiations could be undertaken to address authentication aspects specifically with Canada's most important trading partners. **(http://e-com.ic.gc.ca/english/releases/41d12.html)** and **(http://pm.gc.ca/default.asp?Language=e&Page=publications&Sub=newsreleases&Doc=news_re19991216 1119_e.htm)**

[26] An industry-led collaboration created to accelerate the adoption of Public Key Infrastructure technology and PKI-based solutions as the trusted foundation for secure e-business applications. **(http://www.pkiforum.org)**

The development of a framework will also assist users in making important choices. In a competitive market, consumers would normally choose CAs based on performance and cost that would, in most cases, be spelled out in a contract. However, given the array of technical, business and legal issues associated with the provision of CA services, contracts in this environment maybe be long and complex. This would place an unreasonable burden on the ability of consumers to analyse these contracts, properly distinguish between CAs, and make rational choices. This will be further hindered by the potential need to refer to other lengthy documents such as the certificate policy[27] and certificate practice statement[28] to understand, for example, the CAs approach to mutual recognition or cross-certification. A framework for this relationship will help to promote open and fair competition and ensure that it is based on merit.

e) Market Development Aspects

Providing some and co-ordination for the development and use of electronic authentication services will also help create an environment conducive to strengthening the competitive position of both large and small businesses in this marketplace. Canada is already a significant player in the security products and services segments of the electronic commerce market, but providing some co-ordination to the development and use of these services and promoting their use broadly across all sectors will provide for Canada to enjoy the opportunities and jobs and growth benefits that are available.

2.2 Proposed Scope of Framework

It is intended that the framework will address business-to-business and business-to-consumer aspects of electronic commerce. The business-to-government and government-to-business components are the purview of the Treasury Board Secretariat in the context of its role to design, develop and co-ordinate the Government of Canada Public Key Infrastructure[29] (as well as other departments who opt for other approaches to meet specific

---

[27] A certificate policy indicates the applicability of a certificate to a particular community and/or class of application. It also defines the parties and their relationships and obligations to each other.

[28] A certificate practice statement sets out the procedures a CA will use to issue and manage certificates. Where the certificate policy can be thought of as the "what", the certificate practice statement can be thought of as being the "how".

[29] Commonly known as the "GOC-PKI". A PKI uses public keys and digital signatures to provide for confidentiality of information, authentication of actors, integrity of data, non-repudiation of actions, and access control. The GOC-PKI will provide a uniform key management and key certification process across the government. **(http://www.cio-dpi.gc.ca/pki/Initiatives/initiatives_e.html)**

requirements). Similarly, citizen-to-government and government-to-citizen[30] aspects fall outside the scope of Industry Canada's work in this area. However, it is recognized that public sector implementations and government business will be influencing factors.

The purpose of the framework is to provide for the development and use of authentication services in Canada. As such, the framework will need to recognize and support the benefits of choice and freedom of contract by allowing parties to determine the terms and conditions best suited to their transaction or communication. On this basis, it is not intended to preclude or interfere with contract-based approaches but rather to provide for some commonality, predictability and confidence for users of these services.

Finally, the framework will ideally be technology and architecturally neutral. However, given the predominance and profile of public key approaches to address secure electronic commerce requirements, there could be aspects that may need to focus on public key approaches to ensure meaning and applicability to the reality of the current environment.[31] In doing so, however, there would be no intention to preclude the use of other technologies or the review of this framework in light of new technology advances.

---

[30] Referred to as "Government On-Line" or "GOL". The project involves providing Canadians with access to government information and services on-line.

[31] While one of the objectives of this work is to remain technology neutral, this goal has proven problematic in some fora. For example, while the UNCITRAL initially adopted a technology neutral approach in preparing rules that provide for more certainty when particularly reliable technology is used for signing, the work is now focussing on digital signatures (those created with public key cryptography) since it is the best known of methods at this time.

Part 3 - Authentication & Certification Services - Proposed Approach

3.1 General

Consultations to date have determined that stakeholders are interested in establishing a co-ordinated approach to trust. While there has, as yet, been no elaboration on the precise nature and extent of any co-ordinated approach, most have agreed that some form of common market-based principles for the development and use of authentication services in Canada would be useful. The predominant view is that they should be of a high-level, cross-sectoral nature to provide a level of clarity and consistency to end users, enhance interoperability possibilities and position Canada well internationally. It has been noted that such principles could, in turn, provide the foundation for accreditation of certification authorities.[32] On this basis, the reach and content of the principles require consideration. Potential accreditation models and criteria also need to be explored to identify those aspects (e.g. roles, responsibilities of the various players, etc.) that will need to taken into account in the development of principles.

3.2 Principles

a) General

Guiding principles have been developed by an array of international fora. The *International Consensus Principles for Electronic Authentication,* developed by the Internet Law and Policy Forum (ILPF) [33], are a useful reference for the principles development process in Canada. In addition, ongoing work within the Alliance of Global Business (AGB) and the Global Business Dialogue (GBDe) provides good benchmarks for private sector objectives and expectations globally that will need to be consulted to ensure Canada's approach is compatible with international directions.

Essentially, in all cases, these organizations urge that national approaches respect freedom of contract, seek technology-neutral and architecturally-neutral solutions, and be market-driven. These objectives are consistent with those that have been articulated for this work by Industry Canada in consultation with stakeholders.

---

[32] Accreditation refers to the process of evaluating and certifying the trustworthiness of authentication and certification services. It is generally acknowledged that, in this environment, a necessary element of any framework for authentication services is the accreditation of certification authorities. As such, the concept of accreditation has been incorporated in the work of several key international and industry fora.

[33] A non-governmental forum for informal dialogue and information exchange related to legal and policy issues affecting the Internet and electronic commerce. The principles (April 1999) are intended to facilitate global electronic commerce based on the creation of predictable legal environment for electronic authentication which protects users and reflects their needs. (**http://ilpf.org**)

In addition, some individual industry sectors have also undertaken initiatives in this area that will serve as useful references in developing principles. The *CARAT Guidelines*[34] (a publication of "NACHA" - the National Clearing House Association) may offer a starting point for discussion of the business and legal expectations as well as the relationships and requirements of the various parties involved. These *Guidelines* are particularly useful as they are flexible and generic in nature and thus provide for applicability to a wide range of business models. The *American Bar Association Guidelines*[35] will also be helpful in terms of providing a framework for discussion of the legal aspects.

The work of the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) on a range of WebTrust services is also of interest.[36] Existing and emerging web seal programs may also have implications to the principles.[37]

How can existing work efforts and documents be adopted for use in the development of principles in Canada?

b) Applicability and Scope

Generally, current literature and policy discussions in international fora categorize authentication models on the basis of whether there is contractual privity between the parties. Specifically, it is generally agreed that, where there is contractual privity between parties, it is a "closed model". This is in contrast to "open models", where indirect relationships are typically involved. A range of "hybrids" or "open but bounded" models exist between these two. The introduction of intermediaries into the various models and the varying nature of their possible relationships (e.g.

---

[34] *Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*. Developed under the auspices of The Internet Council, a NACHA-sponsored Council. They are available at: **(http://internetcouncil.nacha.org)**

[35] *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (August 1996). American Bar Association Information Security Committee. **http://www.abanet.org/scitech/ec/isc/dsgfree.html**

[36] *WebTrust Principles and Criteria for Business-to Consumer Electronic Commerce* (October 1999). Available at: **(http://www.cica.ca/cica/cicawebsite.nsf/public/SPASWebtrust)**. *WebTrust Principles and Criteria for Certification Authorities* (February 2000). **(http://WWW.AICPA.ORG/homepage.htm)**.

[37] Of particular interest is the the development of a Canadian "trustmark", proposed by the Canadian E-Business Opportunities Roundtable. The concept is being studied by one of the six teams following up on the recommendations coming out of the Roundtable (in collaboration with the Office of the Consumer Affairs).

agency relationship or simply "conduit" role, etc.) make further variations of the models possible.

Stakeholders have expressed the view that there will be legal questions in this environment, even when contracts are being relied upon, and that, on this basis, both open and closed models would benefit from common parameters. This view has been taken further by others who have noted that, due to the complexity of the contracts that are likely to be required in this environment, there may be too much of an onus on individual users to understand them and make informed choices and comparisons about the various services. On this basis, a set of common principles needs to be applied to all models. However, it has been suggested that implementation details may differ in some circumstances, particularly in the case of closed models.

For example, liability and related aspects may be areas where the applicability of principles may differ in closed models for at least two reasons. First, it has been suggested that closed models should be viewed in the context of the overall business model and that, therefore, risk is distributed throughout the total infrastructure and mitigated by a number of components. Secondly, it has been suggested that closed models may be in a position to manage risk more effectively given they will generally be able to control all aspects of the authentication process. On this basis, it has been advocated that the complete business model, and the security features it incorporates, needs to be assessed when determining the applicability of principles. This is not to say that only particular principles would be relevant in certain circumstances, but rather that the implementation details of each of them may vary. The highly inter-related nature of the issues that the principles will address makes it inappropriate to select only a subset of them.

It is also recognized that models will differ not only on the basis of whether they provide services to open and closed communities, but also on the basis of the level of trust and assurances involved. Thus the requirements of individual applications will determine the appropriate levels of trust and assurance provided by the CA. CAs will also vary in structure and this will need to be taken into account.[38] However, regardless of the array of models and the particular implementation, it can be assumed that all will have certain common basic process and governance requirements. At a minimum, it is these aspects that will need to be addressed on a common basis in the principles if a coherent framework for authentication services is to be the result.

To what extent should the principles influence the terms and conditions of the contracts that will govern authentication-related services in closed environments. Under what circumstances might it be appropriate for implementation aspects of the principles to differ?

c) Content

[38] Some models will involve hierarchical relationships with one root CA and an array of subordinate CAs. Others will involve relationships that involve a "bridge" to various CAs.

Feedback from stakeholders who have participated in this consultation program to date points to many areas that will need to be given consideration in the development of principles. Those aspects that were cited by virtually all stakeholders consulted to date are discussed immediately below:

i) Privacy

Stakeholders have offered the view that any principles developed will need to provide some parameters aimed at ensuring authentication and certification services are ***privacy-respecting***. While the privacy provisions in the new legislation (the *Personal Information Protection and Electronic Documents Act)* will apply to CAs themselves, there will be a need to ensure that derived or secondary processes associated with the services they provide are also privacy-respecting.

ii) Disclosure

Virtually all stakeholders consulted to date have agreed that there is a need for full ***disclosure*** of the rights and responsibilities of all parties. Similarly, full disclosure of risk and liability to all parties in a transaction (users, providers, third parties and relying parties) will also presumably be an important component of the principles. This will be particularly critical in the context of applications and implementations employing non-repudiation functionality.[39]

iii) Liability

The uncertainty surrounding liability has been raised frequently by stakeholders. They suggest that ***liability guidelines*** should perhaps be developed for these services. Specifically, the majority have suggested that the extent to which CAs can limit or exempt their liability for losses arising from the use of their certificates by relying parties should be broadly addressed in any principles. Some even felt that minimum levels of liability on the part of CAs should be specified with immunities somehow defined.[40]

What other areas should the principles address? And why?

---

[39] The high rates of repudiated transactions experienced in current Internet-based credit card transactions suggest that consumers will need to be made fully aware of those implementations. Flexibility may not exist if non-repudiation functionality has been deployed.

[40] Additional dimensions could be added to this discussion if it was determined that some base liability "zones" should be established since there would probably be a need to have them differ on the basis of whether business- to-business or business-to-consumer transactions are involved.

d) Adherence

While it is understood the principles would be non-binding and voluntary, most stakeholders have suggested that some form of adherence mechanism(s) will be necessary. However, there is debate as to what form this should take and it may well be that a variety of approaches is appropriate depending on then nature of the service provided by the CA and whether open or closed models are involved.

Some stakeholder groups maintain that the only effective approach would be to require reviews by independent bodies and suggest that existing entities with an auditing function may be well positioned to apply it to this environment.[41] Others are of the view that any requirement for independent reviews has the potential to be a cost barrier[42] and consider more of an industry self-regulatory approach to be desirable. Such an approach could involve self-declarations of conformance to the principles, perhaps backed by penalties and liability for non-adherence. Adopting this approach would have implications to other elements of the principles (e.g. full disclosure of information would need to be a requirement).

It is also possible that the necessary assurances about players can be derived from the establishment of a series of "high-level" authorities (e.g. existing trusted entities or regulated entities could be established as CAs) and would be derived through cross-certification (or mutual recognition arrangements) with these high-level authorities. However the competition dimensions of adopting this particular alternative would need to be examined.

Those who do not believe a compliance component is necessary have suggested that use in the marketplace should be the test on the assumption that inadequate or inferior implementations simply will not survive. However, this approach assumes a certain level of understanding of the technology by users that is perhaps not there.

---

[41] There are already industry initiatives underway in this regard. For example, the American and Canadian Institutes of Chartered Accountants have produced an exposure draft entitled: *WebTrust Principles and Criteria for Certification Authorities* that provides a framework to assess the adequacy and effectiveness of the controls employed by CAs. (*WebTrust Principles and Criteria for Certification Authorities* (February 2000) **(http://WWW.AICPA.ORG/homepage.htm)**.

[42] However, it has been suggested by stakeholders that a barrier of this nature would potentially be viewed beneficially by consumers on the basis that it would minimize the possibility of having "fly-by-night" CA offerings.

How should adherence be addressed? Under what circumstances is some form of third party evaluation or verification of the principles desirable? Who should provide the evaluation function? On the basis of what criteria? What are the implications of basing compliance on self-declarations? Under what circumstances might it be appropriate to derive the necessary assurances from relationships with existing trusted entities?

e) Role of public sector CAs *(in particular the GOC-PKI)*

In the context of its commitment to provide innovative service delivery to Canadians and to improve the efficiency of government operations using information technology, the Government of Canada (GOC) has implemented a government-wide security architecture for electronic service delivery. A public key infrastructure (PKI) has been developed to provide for the confidentiality, data integrity, authentication and non-repudiation features needed for enhanced privacy protection and to secure electronic transactions. This infrastructure provides the security and confidence needed to conduct the electronic business of government.

To the extent that government business requires interaction with the private sector, and to the extent that market demand for access to government electronic services may drive the need for private sector authentication service providers, the relationship of the GOC-PKI to this work will need to be kept in mind. In particular, the cross-certification criteria and procedures[43] that have been developed for CAs wishing to "interwork" with the GOC-PKI may have a potential role to play in the development of the principles (particularly in the context of the principles providing the foundation for accreditation of private sector CAs).[44] The GOC-PKI criteria and procedures may also be important from the perspective that they be may be followed by provincial PKIs in the future.

f) Mechanism for Developing Principles

Options for mechanisms for developing the principles would include using an existing industry association with representation augmented (for the purposes of this work) to include other industry sectors and governments. Alternatively, it may be determined that a new forum should be established expressly for the purpose of addressing this (and perhaps other)

---

[43] *Canada Public Key Infrastructure : Cross-Certification Methodology and Criteria* (September 1999). See **(http://www.cio-dpi.gc.ca/pki/Documents/documents_e.html)**

[44] Relationships with public sector CAs could offer the private sector alternatives to becoming accredited under an industry-led scheme. For example, the Australian approach recognizes the transference of trust if an entity cross-certifies with its national "GATEKEEPER" strategy for public key use in the Government. **(http://www.gpka.gov.au/)**

aspects of authentication.[45]

Regardless of the precise nature of the forum used, the development work on principles will need to have broad participation and input to provide for the interests and requirements of all stakeholder groups to be considered. The challenge will be to balance these interests and manage the competition dimensions (see Section 4.1c). Since stakeholders have expressed the view that much of the forward agenda for authentication requires public/private sector collaboration, this is an area where active public sector involvement is desirable in terms of helping to ensure a balanced and neutral process.

Is there a need to establish a new forum for this work? Who should establish this forum? Who should be involved? What roles should they play?

3.3 Principles as a Basis for Accreditation

A set of principles will provide a framework for basic components of accreditation of CAs. As such, it is useful to examine potential accreditation criteria and models to identify those aspects (e.g. roles, responsibilities of the various players, etc.) that will need to taken into account in the development of principles.

While there are various approaches to accreditation, all models will involve the interaction of a variety of players, each with a role, or a combination of roles. In ***Appendix B***, a number of possible roles are identified and named. While it is recognized that not all these roles will be appropriate in every business model, and that there may be other roles that have not been identified, the model is intended to provide a point of departure from which to consider how the functions and obligations of the parties might be allocated. On this basis, it is not a recommended or preferred model, but rather an illustrative one to provide a framework for discussion in the context of the development of principles.

Any form of accreditation will generally involve ensuring that the level of security, legal and performance requirements (as set out in principles and potentially in tandards) are effectively met by a CA in its certificate policy. Accreditation can also confirm (usually through independent verification) that the CA practices developed and documented in the certificate practice statement comply with the requirements in the certificate policy and (possibly through compliance

---

[45] This has been the approach taken by some jurisdictions. For instance, in Australia, the National Electronic Authentication Council (NEAC) was established to provide a national focal point on authentication matters including co-ordinating authentication-related activities at a national and international level, providing advice to government and monitoring market developments. The Council includes representation from major organizations with an interest in the emerging authentication environment (users, industry and government organizations). **(http://www.noie.gov.au/projects/consult/NEAC/index.htm)**

audits or levying of penalties), ensure the CA follows disclosed practices. An even more expanded approach would incorporate mechanisms to also "accredit" the evaluation mechanisms.[46]

There are already tools that have been developed in the marketplace which serve as a foundation for accreditation. In particular, PKIX Part 4 *Certificate Policy and Certification Practices Framework* (developed under the auspices of the Internet Engineering Task Force)[47] offers a checklist for certificate policy requirements (pertaining to certificate generation and revocation, maintenance of records etc.) and for aspects of certificate practice statements (such as identity requirements, key generation, certificate issuance etc). It has been a widely-used tool in North America for accreditation initiatives.

What common accreditation criteria are desirable? (See Appendix B for an illustration of how functions and obligations might be allocated in accreditation schemes.) Are the roles identified in Appendix B applicable and appropriate for the Canadian environment? Where might your organization have a role (or roles) in this model?

[46] However, it has been suggested that this would not be required if evaluations were conducted by entities already recognized as trustworthy (e.g. legal firms, chartered accountancy firms etc.).

[47] *Internet X.509 Public Key Infrastructure Policy and Certification Practices Framework.* **(ftp://ftp.isi.edu/in-notes/rfc2527.txt)**

Part 4 - Market Development: Opportunities and Challenges

Defining a framework for authentication services in Canada should be complimented with initiatives to promote its development and use. This section of the paper identifies the challenges associated with promoting the use of authentication and seeks input as to how we can increase deployment and adoption rates of effective authentication techniques. It also explores a range of strategic initiatives that can be undertaken to address the challenges and capture the opportunities in this marketplace. Finally, in the course of discussing these aspects, this section raises a number of issues that will require consideration in the development of principles.

Taking into account input received from stakeholders to date, Industry Canada's current perspective is that market development initiatives should:

- promote the adoption and use of electronic authentication by businesses and consumers;
- encourage competition and foster innovation in new technologies and applications; and,
- expand domestic and international opportunities for suppliers and end users of authentication and certification services.

4.1 Promoting the Adoption and Use

a) Position as a strategic investment

Business will need to understand that electronic authentication offers the functionality for interactive communication over open networks. Stakeholders have observed the need to encourage business to take a forward-looking view and recognize that robust authentication techniques will meet the expectations that users have about how technology can improve their lives.

Thus, the investment needs to be positioned as one of a strategic nature that will allow businesses to remain competitive, and to some extent, anticipate demand. In addressing its strategy to accelerate Canada's participation in the Internet economy, the Canadian E-Business Opportunities Roundtable's forward workplan has already provided opportunities to communicate the benefits of investment in this area.[48] Undertaking specific targeted initiatives at the industry association level may be useful.

---

[48] The Roundtable's forward action plan called for a series of regional outreach events to raise awareness and encourage adoption of electronic commerce. Discussion of authentication has been incorporated into some of these events. For more information on these events see **(http://e-com.ic.gc.ca/eteam/events.html)**.

While this technology needs to be recognized and promoted as a critical enterprise security investment, business will also need to understand how it can add value to their business processes. Specifically, they will need to understand how strong authentication techniques can support and enable new applications and thus, provide new revenue streams. On this basis, promotional efforts should concentrate on positioning security as an enabler of new business processes. The profiling and communication of success stories would be helpful in this regard.

Questions have been raised about the economic viability of the use of robust authentication techniques. Some stakeholders are of the view that there is simply no business case for the technology while others feel the business case has yet to emerge. Those expressing the latter view are certain that many more businesses and consumers would embrace electronic commerce if they had assurances that their transactions were secure. They believe that increased use will build the business case.

In raising business awareness and encouraging investment in the technology, the need for thorough risk assessments will need to be emphasized. It is possible that generic, or sample frameworks for developing risk management models may assist in this regard, particularly in the case of small enterprises that find challenges in taking this on. Such an initiative could be done on a collaborative basis with industry associations.

Other inhibitors to investment will also need to be addressed. Based on current pricing structures, the cost of deployment would appear to be one such inhibitor. The significant nature of the ongoing maintenance costs is also part of the business equation. On this basis, business will need to be encouraged to contemplate the range of security levels possible and the "stepped" or phased approaches to strong solutions that are possible. On a related note, any strategic initiatives undertaken to increase deployment rates will likely need to address the means by which legacy systems can be re-engineered to provide robust authentication. The supplier community would appear to have an opportunity to provide pathways or "routes" to strong authentication in this regard.

What strategic measures need to be adopted to promote the benefits of strong authentication techniques? Are there public sector initiatives that could complement private sector undertakings?

b) Raising consumer awareness and use

In the consumer context (and often in the context of small and micro businesses), there will be challenges in raising awareness and adoption rates. Consumer surveys continue to indicate that privacy and security are important concerns and, while consumers are willing to try buying goods

and services, their continued buying activity depends on the relative ease and success of their preliminary buying experiences. Emerging statistical trends show that consumers are actually engaging in a form of "balancing" exercise when it comes to on-line activity. With respect to privacy, there appear to be large numbers of consumers willing to trade off some aspect of gain (e.g. bonus points, contest entry etc.) for allowing businesses access to certain personal information. However, with the passage of the *Personal Information Protection and Electronic Documents Act,* they can now do so knowing there will be privacy protection measures in place limiting the use and disclosure of this information and that oversight by the Office of the Privacy Commissioner is an element of these measures.[49] With respect to security, many consumers lack an understanding of the various security techniques that are available, and thus accept current basic security implementations for reasons associated with convenience and cost. However, these trends are largely based on general observations. At this point in time and the marketplace is, as yet, not well-informed about the precise nature of the privacy and security trade-offs consumers are willing to make.

There will also be challenges related to the consumer interest in having transparent solutions. Consumers will need to have some level of understanding of the technology if they are to understand certain features and compare implementations in order to make informed choices between competitive CA offerings. Although the pricing structures for this marketplace are yet to emerge, there would also be a need for a certain level of understanding of the technology on the part of consumers if they are faced with making choices where cost is a factor. There will also be a need to explain the non-repudiation functionality offered by the technology. The current rates of repudiated transactions conducted over open networks suggests that this is an alternative that consumers are relying on. In the context of strong authentication techniques where non-repudiation functionality is deployed, it will be important that all parties are fully aware of their separate rights and responsibilities.

There may also be a need to manage other aspects of consumer acceptance. In particular, stakeholder consultations have revealed that there is a perception that the use of electronic authentication offers the opportunity to enhance consumer protection to "raise the bar". While this may be the case, certain responsibilities and accountabilities will remain. For example, users will need to understand that they have a responsibility to keep their private key secure. Since the consumer experience has been that they are often expected to take on more liability and responsibility with advances in technology (e.g. their responsibility to remember personal identification numbers or "PINs" and manage their secrecy and their

---

[49] In some instances, where legislation of a substantially similar nature has been adopted at the provincial level, it will be that legislation that will provide the protection.

liability for transactions if this is not done properly) there may in fact be a degree of skepticism for the use of digital certificates. This suggests that mechanisms to ease the burden of managing certificates and the fair allocation of liability will be important.

It has been generally understood that governments have a role in educating and empowering the public to enhance awareness of their responsibilities and their ability to exercise choice with respect to their protection as consumers. The various public/private sector collaborative initiatives being undertaken by Industry Canada's Office of Consumer Affairs (OCA) in the area of electronic commerce[50] confirms that this has already been recognized by the Federal Government and is being acted upon. As previously discussed, it is possible that synergies or opportunities for joint work may be possible in addressing the authentication agenda.

How can strong authentication be promoted to the business community as being a strategic investment? By whom? How can consumer awareness of the benefits of strong authentication techniques be improved?

c) Encouraging competition and fostering innovation

Competitive concerns in electronic markets are similar to those found in traditional markets tempered by a number of special characteristics (e.g. new roles for players, introduction of intermediaries, rapid growth of the market, etc.). In the authentication and certification services environment, competition aspects may arise that will need to be monitored[51]. While some of these have been explored in Section 2 (*Defining the Forward Agenda*), others relate more to market development aspects and are discussed below.

Some stakeholders expressed concern that, in the context of business-to-consumer electronic commerce, consumers will be required to be "certified" by a particular CA if they want to do business with a particular organization. On the business-to-business side, concern was expressed that there is the potential for businesses to be shut out of procurement processes unless they employ a certain technology or use the services of a certain CA.

---

[50] Notably, the development and publication of *Principles for Consumer Protection in Electronic Commerce - A Canadian Framework* (November 1999) and supporting documentation for merchant and consumer use. More recently, OCA has been working with the private sector to "operationalize" the principles and explore ways to ensure that seal programs meet the principles and provide consumers with the confidence they need to shop on-line. OCA also continues to work with provincial and territorial governments, consumer organizations and industry to raise awareness and educate consumers.

[51] For information about competition law in Canada see **(http://strategis.ic.gc.ca/SSG/ct01250e.html)**. Guidance on complying with competition law can be obtained from the Bureau of Competition Policy.

In the business-to-consumer market, consumer groups have observed that CAs have the potential to assume powerful social roles given that they will be in a position to compile data trails on activity.[52] Specifically, it has been observed that CAs could exercise a great deal of market power respecting individuals choice by virtue of their function in issuing and revoking certificates. It has also been observed that a CA will probably be able to record everyone with whom an individual transacts using a particular digital signature.[53] Some protection and assurances already exist if entities that already function today as "trust agents" become CAs (e.g. financial institutions, accountancy firms, consumer organizations, etc.), but there may be some public policy challenges associated with new players.[54] While significant aspects of these challenges can be addressed through the development and application of marketplace principles, there is a need to remain cognizant of these concerns.

It has also been suggested that there are also public policy issues at the design level of these services and that there is a need to develop services that meet the needs of all players and not just the dominant players (e.g. the service providers). This suggests that there may be a monitoring role for governments on this issue, as well as the closely related matters of pricing of services.

On this basis, stakeholders have suggested that there may be a role for governments as "referees" in this regard but cautioned that it would be highly undesirable to compromise innovation, either by erecting any artificial barriers to entry, or allowing incumbent competitors to erect barriers that would handicap innovative rivals. Care must also be taken to avoid the creation or abuse of power circumstances, whereby private-sector forces could impede the development or growth of the market through exclusionary conduct, either collective or unilateral.

---

[52] This may also be the case in some business-to-business implementations.

[53] This potential arises from the CAs management of revocation lists. Depending on the implementation, those relying on a digital signature may check the revocation list each time. In the process of checking the list, there is the potential for a data trail to be created that would show every inquiry about that particular certificate.

[54] Significant aspects of these challenges can be addressed through the development and application of marketplace principles.

In addressing the competition aspects, there is a need to ensure the marketplace fosters innovation and investment. It has been suggested that commercially viable standards (developed by the private sector) can go a long way towards achieving this goal by providing a level playing field as long as the standards reflect consensual agreement among stakeholders and do not stifle competition and innovation.

Is there a need for special measures in this marketplace to ensure competition and foster innovation? Are there particular concerns with competition dimensions that need to be identified and monitored?

Part 5: Conclusions and Next Steps

There are many dimensions to this work with many inter-related factors coming into play. As efforts aimed at developing a framework for Canada move forward, there will be a constant need to take into account these dimensions, factors and related initiatives and work efforts, both domestically and internationally. While this paper has attempted to provide information on these considerations, this environment is such that developments occur daily. On this basis, the challenge will be to keep abreast of private and public sector developments to ensure the directions taken are in synch with the private and public sector global patterns in this arena.

5.1 Proposed Next Steps

As a next step, the public and private sectors should work on a collaborative basis to:

i) Establish and enable a process for defining a set of common market-based principles applicable to authentication and certification services in Canada.

ii) Plan and implement strategic initiatives aimed at promoting the use of strong authentication techniques among business and individual end users.

iii) Continue to work internationally to influence directions and ensure Canada is well-positioned to take full advantage of the opportunities in this marketplace.

Ongoing public/private sector dialogue has been identified by stakeholders as being essential to advancing the trust agenda in Canada and will be important to the success of the framework development process and taking advantage of market development opportunities. As the next step in this dialogue, stakeholder groups are encouraged to provide responses to any or all of the questions contained in this paper as described at the front of this paper (page ii). ***Appendix C*** has been developed to provide a single point of reference for the questions upon which views and input is sought. Input is also sought on the summary of potential roles in ***Appendix D.***

Appendix A

Authentication Consultation Program: Stakeholder Participants

Academia (Dalhousie University, University of Ottawa)
AEPOS Technologies Corporation
Alliance of Manufacturers and Exporters Canada
Auditor General
Bank of Montreal (MBANX)
BCE Emergis Inc.
Bell Canada
British Columbia Technology Industries Association
Canada Post Corporation
Canadian Association of Internet Providers (CAIP)
Canadian Bankers Association (CBA)
Canadian Council for International Business (CCIB)
Canadian Federation of Independent Business (CFIB)
Canadian Health Coalition
Canadian Imperial Bank of Commerce (Identrus)
Canadian Institute of Chartered Accountants (CICA)
Canadian Life and Health Insurance Association (CLHIA)
Canadian Marketing Association (CMA)
Canadian Payments Association (CPA)
Consumers' Association of Canada (CAC)
DataPrivacy Partners Ltd.
Deloitte & Touche
Electronic Commerce Canada
Entrust Technologies Ltd.
Ernst & Young
IBM Canada Ltd.
Information Technology Association of Canada (ITAC)
KPMG
Mondex Canada
Nortel Networks
Option consommateurs
Privacy Commissioner of Canada (Office of the)
Provinces (British Columbia, New Brunswick, Ontario, Quebec)
Public Interest Advocacy Centre (PIAC)
Retail Council of Canada (RCC)
Royal Bank
Scotiabank
Sprint Canada
Standards Council of Canada
VISA Canada Association

Appendix B

Proposed Framework for Discussion of Accreditation Model(s)

Accreditation Roles and Interaction

While terminology may vary across the international jurisdictions, there is an evolving recognition that accreditation of CAs would somehow involve interaction of players, legal entities, parties, actors, bodies or agents having the following roles:

Competent Authority – An agent of the legal jurisdiction or community of interest. It is responsible, within the jurisdiction or community of interest, for a number of actions which could include some or all of the following:

- Defining the policy and legal environment within which the scheme must operate;
- Negotiating with other *Competent Authorities* to ensure harmonization across legal jurisdictions;
- Issuing licences, authorization, regulations or other government or legal recognition to various CAs ;
- Setting minimum policy requirements for advancing the compatibility of digital signature levels of trust and CA accreditation approach across legal jurisdictions;
- Giving formal recognition to standards, criteria and frameworks for advancing the compatibility of digital signature levels of trust and accreditation approach across legal jurisdictions;
- Approving and giving formal recognition to accreditation approach; and
- Giving formal recognition to a *CA Evaluator Accreditation Body*, which is chartered to carry out the accreditation of *CA Evaluators*.

CA Evaluator Accreditation Body – An independent body, industry association or other agency which could be recognized by the *Competent Authority* or could function on the basis of trust relationships with *CA Evaluators* or *Policy Authorities*. Responsible for:

- Approving and giving formal recognition that *CA Evaluators* are professionally competent to perform evaluations of compliance to Certificate Policies or other requirements which may be provided by the *Competent Authority*; and
- Sanctioning, selecting and/or developing policy compliance evaluation guidance, criteria and standards.

CA Evaluator – An independent agent, member of an accounting body, or other qualified professional which is trusted by the *Policy Authority*. The *CA Evaluator* could be formally recognized by the *CA Evaluator Accreditation Body* if such an entity existed in that jurisdiction or community of interest. Responsible for:

- Evaluating the CA *Operational Authority's* compliance to the Certificate Policy; and

- Using specific evaluation guidance, criteria and standards sanctioned by the *CA Evaluator Accreditation Body*, to develop an "audit opinion" that –

  1) there are adequate controls in place; and

  2) these controls are operating effectively, such that reliance can be placed on transactions that are recorded, processed, executed or maintained by the *Operational Authority* in question.

- Evaluating other evidence of compliance with the target Certificate Policy, where the parties have effected obligations through mechanisms such as contracts and membership agreements and through the implementation of related operational safeguards or business methods. Documentation for such mechanisms need not have been directly incorporated into the Certification Practice Statement. For specific Certificate Policy requirements, an external reference may be sufficient to convey an understanding to the *CA Evaluator*, of the relevant material practices of a closed community CA domain;

- Producing a Certificate Policy Compliance Evaluation Report. The potential users of an evaluation report include:

  a) **Relying parties** have a significant interest in knowing that a scheme's practices operate with sufficient effectiveness to achieve the requirements within the Certificate Policy;

  b) **Subscribers** have an interest in knowing that the CA is meeting the requirements of the Certificate Policy;

  c) **Competent Authorities** - An audit is an important component of any authorization, regulation, licensing or other recognition process. The *Competent Authority* would utilize the evaluation report as part of the initial and on-going recognition process; and

  d) **Policy Authorities** are a primary user of the evaluation report, as the audit is one of the requirements of the target Certificate Policy and it demonstrates the CA's compliance with that policy. The evaluation report would also be used by Policy Authorities in any cross-certification negotiations; and

  e) **Operational Authorities.** While the evaluation report is not intended to provide recommendations for improvement in the internal controls of a certification authority, a value-added benefit of the CA compliance evaluation would often include observations of the auditor for improvements in operations.

Security Accreditation Authority – An agent of the CA domain or enterprise. Responsible for:

- Approving the operation of the CA in a particular mode using particular safeguards; and

- Accepting residual security risks on behalf of the CA domain or enterprise.

Policy Authority – An agent of the CA domain or enterprise. The *Policy Authority* is responsible for:

- Selecting and/or defining documentation for use in the CA domain or organizational enterprise;
- Approving any cross-certification or interoperability agreements with external domains;
- Approving practices which the CA must follow by reviewing the Certification Practice Statement to ensure consistency with the Certificate Policies; and
- Providing policy direction to the *Operational Authority.*

Operational Authority – An agent of the CA domain or enterprise. In some business models, there might be several Operating Authorities involved in the process of generating a certificate. In most cases, all elements would be accredited to establish the required level of trust for a particular certificate. The *Operational Authority* is responsible to the *Policy Authority* for:

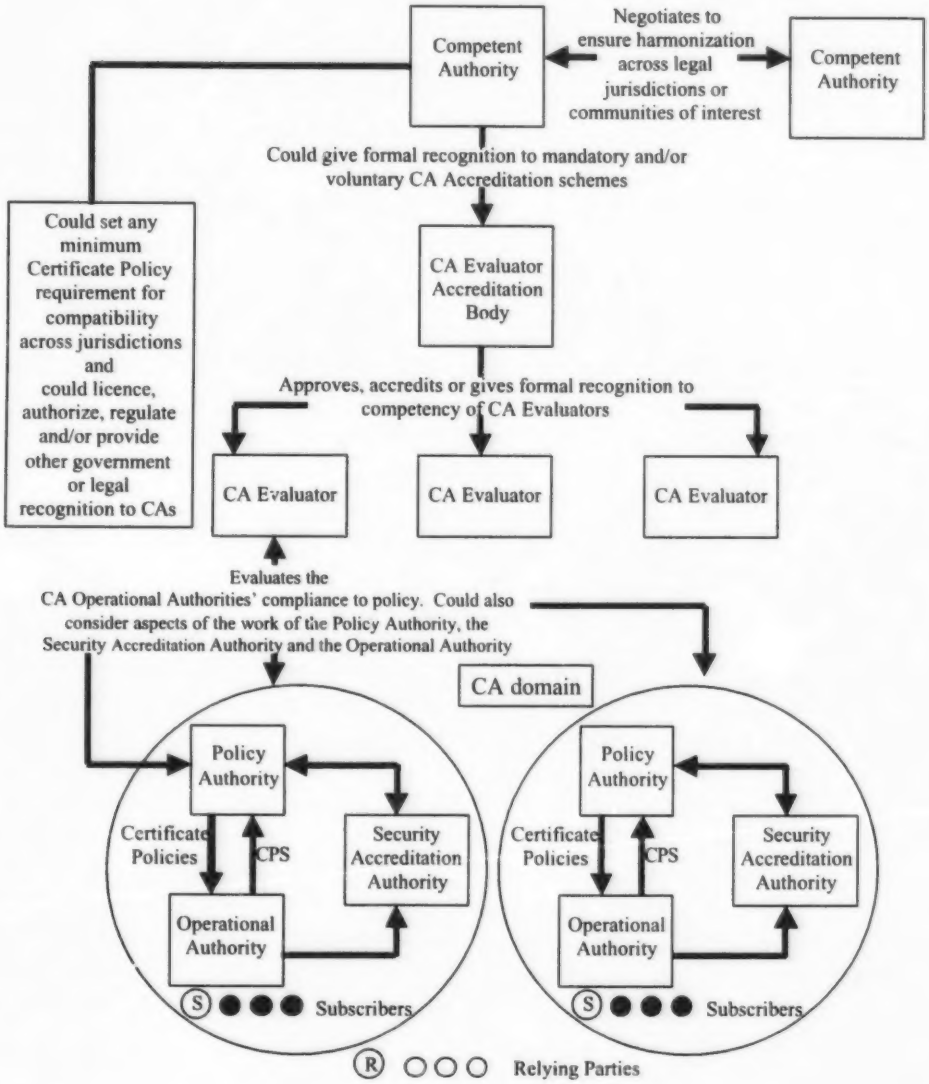
- Interpreting the Certificate Policies which were selected or defined by the *Policy Authority;*
- Developing the practices documenting compliance to the policies and other requirements;
- Ensuring that the practice statements are updated as required; and
- Operating the CA or scheme in accordance with the practice statements.

Subscriber – A member of the CA domain. A party who is the subject of a certificate and who is capable of using, and is authorized to use, the private key, that corresponds to the public key in the certificate. Responsibilities and obligations of the *Subscriber* would be as required by the CA's policy.

Relying Party - May or may not be *Subscriber* of the same domain. The *Relying Party* is a recipient of a certificate who acts in reliance on those certificates and/or digital signatures verified using that certificate.

Accreditation Framework

The following diagram illustrates the relationships between the various roles. To accommodate either the needs of the legal jurisdiction and/or closed and open business models, unique CA accreditation models can be postulated by combining roles.


Competent Authority
Negotiates to ensure harmonization across legal jurisdictions or communities of interest
Competent Authority
Could give formal recognition to mandatory and/or voluntary CA Accreditation schemes
Could set any minimum Certificate Policy requirement for compatibility across jurisdictions and could licence, authorize, regulate and/or provide other government or legal recognition to CAs
CA Evaluator Accreditation Body
Approves, accredits or gives formal recognition to competency of CA Evaluators
CA Evaluator
CA Evaluator
CA Evaluator
Evaluates the CA Operational Authorities' compliance to policy. Could also consider aspects of the work of the Policy Authority, the Security Accreditation Authority and the Operational Authority
CA domain
Policy Authority
Certificate Policies
CPS
Security Accreditation Authority
Operational Authority
S
Subscribers
Policy Authority
Certificate Policies
CPS
Security Accreditation Authority
Operational Authority
S
Subscribers
R
Relying Parties

© Industry Canada and LGS Group, 1999. All rights reserved.

Appendix C

Summary List of Questions

Authentication & Certification Services - Proposed Approach

Principles

1) How can existing work efforts and documents be adopted for use in the development of principles in Canada?

2) To what extent should the principles influence the terms and conditions of the contracts that will govern authentication-related services in closed environments. Under what circumstances might it be appropriate for implementation aspects of the principles to differ?

3) What other areas should the principles address? And why?

4) How should adherence be addressed? Under what circumstances is some form of third party evaluation or verification of the principles desirable? Who should provide the evaluation function? On the basis of what criteria? What are the implications of basing compliance on self-declarations? Under what circumstances might it be appropriate to derive the necessary assurances from relationships with existing trusted entities?

5) Is there a need to establish a new forum for this work? Who should establish this forum? Who should be involved? What roles should they play?

Principles as a Basis for Accreditation

6) What common accreditation criteria are desirable? (See Appendix B for an illustration of how functions and obligations might be allocated in accreditation schemes.) Are the roles identified in Appendix B applicable and appropriate for the Canadian environment? Where might your organization have a role (or roles) in this model?

Market Development: Opportunities and Challenges

7) What strategic measures need to be adopted to promote the benefits of strong authentication techniques? Are there public sector initiatives that could complement private sector undertakings?

8) How can strong authentication be promoted to the business community as being a strategic investment? By whom? How can consumer awareness of the benefits of strong authentication techniques be improved?

9) Is there a need for special measures in this marketplace to ensure competition and foster innovation? Are there particular concerns with competition dimensions that need to be identified and monitored?

Appendix D

Summary of Potential Public/Private Sector Roles

Shared Private/Public Sector

- Promote the use of authentication and related services as the trusted, secure foundation for electronic commerce.
- Communicate the benefits of the technology and enhance user awareness and understanding.
- Educate consumers and business on the technology and its benefits.
- Establish a common approach to the accreditation of certification authorities.

Private Sector

- Develop and implement accreditation schemes.
- Develop a broad set of marketplace principles.
- Provide input to international activity aimed at ensuring Canada's approach is compatible with global directions and that Canadian certificates are recognized globally.
- Provide leadership through the development of products that meet user requirements.
- Provide timely input to Canadian governments on policy objectives and strategies.
- Develop standards (as required) to underpin the principles and enhance interoperability.

Public Sector

- Facilitate dialogue on domestic approaches linking to international.
- Facilitate principles development initiative.
- Co-ordinate with the provinces.
- Monitor competition dimensions (and address if required).
- Be a model user (e.g. GOC-PKI).
- Establish dialogue and liaison with the academic community.
- Protect Canadian interests (ensure that any approach adopted allows for Canadian consumers and business to interoperate internationally).
- Develop preparatory responses (should private sector solutions fail).

List of Abbreviations

ABA	American Bar Association
AGB	Alliance of Global Business
APEC	Asia-Pacific Economic Cooperation
BCG	Boston Consulting Group
BCP	Bureau of Competition Policy
BIAC	Business and Industry Advisory Committee (to the OECD)
CA	Certification authority
CARAT	Certification Authority Rating and Trust (Task Force) - NACHA
CIO	Chief Information Officer
EU	European Union
GBDe	Global Business Dialogue
GOC	Government of Canada
GOC - PKI	Government of Canada Public Key Infrastructure
GOL	Government On-line
IETF	Internet Engineering Task Force
ILPF	Internet Law Policy Forum
NACHA	National Automated Clearing House Association (United States)
NEAC	National Electronic Authentication Council (Australia)
OCA	Office of Consumer Affairs (Industry Canada)
OECD	Organization for Economic Co-operation and Development
PIN	personal identification number
PKI	public key infrastructure
PKIX	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
PSCIOC	Public Sector Chief Information Officers Council
TBS	Treasury Board Secretariat
UECA	Uniform Electronic Commerce Act
ULCC	Uniform Law Council of Canada
UNCITRAL	United Nations International Commission on International Trade Law

Selected Sources

Domestic - Background

- *Minister Manley Outlines Canadian Cryptography Policy*, Industry Canada, October 1998
  http://e-com.ic.gc.ca/english/releases/41d6.html
- *Speaking Notes for the Honourable John Manley - Presentation to the National Press Club - Canada's Cryptography Policy*, Industry Canada, October 1998
  http://e-com.ic.gc.ca/english/speeches/42d3.html
- *Summary of Canada's Cryptography Policy*, Industry Canada
  http://e-com.ic.gc.ca/english/fastfacts/43d7.html

Domestic - Electronic Commerce Branch Consultation Program

- *Electronic Authentication: Summary of Findings of Bilateral Consultations*, October 1999
  http://e-com.ic.gc.ca/english/documents/bilat-eng.pdf
- December 6, 1999 Electronic Authentication Policy Workshop Documentation:
  - Agenda
    http://e-com.ic.gc.ca/english/documents/agenda.pdf
  - Summary Report
    http://e-com.ic.gc.ca/english/documents/wkshp-rpt.pdf
  - Working Papers
    http://e-com.ic.gc.ca/english/documents/workingdocs.pdf

Domestic - Related Initiatives and Reference Documents

- *Approaches to Authentication,* AEPOS Technologies Corporation, December 1999.
- *Australia-Canada Joint Statement on Global Electronic Commerce*, Governments of Australia and Canada, February 2000
  http://e-com.ic.gc.ca/english/releases/41d12.html
- *The Personal Information Protection and Electronic Documents Act*, Industry Canada, April 2000
  http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html
- Canadian Institute of Chartered Accountants (CICA) (About WebTrust Services)
  http://www.cica.ca/cica/cicawebsite.nsf/public/SPASWebTrust
- *Certification and Accreditation for PKIs and Certification Authorities - Survey of Standards, Trends and Identification of Potential Models*, Domus Software Limited/Industry Canada, August 1998.
- Department of Justice Canada (Programs and Services - Electronic Commerce)
  http://canada.justice.gc.ca/en/ps/ec/index.html

- *European-Union Canada Joint Statement Electronic Commerce in the Global Information Society*, European Union and the Government of Canada, December 1999
  http://e-com.ic.gc.ca/english/71ta.html
- *Government of Canada Public Key Infrastructure* (GOC PKI), Treasury Board Secretariat
  http://www.cio-dpi.gc.ca/pki/Initiatives/initiatives_e.html
- *Principles of Consumer Protection for Electronic Commerce - A Canadian Framework* (and supporting documentation), Industry Canada, Office of Consumer Affairs, November 1999
  http://strategis.ic.gc.ca/SSG/ca01180e.html
- Public Sector CIO Council (PSCIOC)
  http://www.tbs-sct.gc.ca/cio-dpi/pscioc/pscioc_home_e.html
- *Fast Forward: Accelerating Canada's Leadership in the Internet Economy* - Report of the Canadian E-Business Opportunities Roundtable, The Boston Consulting Group (Canada), January 2000
  http://www.bcg.com/practice/ecommerce_canadian_roundtable.asp and/or
  http://e-com.ic.gc.ca/eteam/resource.html
- *Uniform Electronic Commerce Act*, Uniform Law Conference of Canada
  http://www.law.ualberta.ca/alri/ulc/eindex.htm

International - Related Initiatives and Reference Documents

- Business and Industry Advisory Committee to the OECD (BIAC)
  http://www.biac.org/
- *Digital Signature Guidelines*, Information Security Committee, Section of Science and Technology, American Bar Association, August 1996
  http://www.abanet.org/scitech/ec/isc/dsgfree.html
- *Directive on a Community framework for electronic signatures*, the European Parliament and the Council of the European Union, December 1999
  http://www.ispo.cec.be/Ecommerce/legal/documents/1_01320000119en00120020.pdf
- *Draft Uniform Rules on Electronic Signatures*, UNCITRAL
  http://www.uncitral.org/english/sessions/wg_ec/wp-84.pdf
- Global Business Dialogue on Electronic Commerce (GBDe)
  http://www.gbd.org/
- International Telecommunication Union (ITU)
  http://www.itu.int/
- International Chamber of Commerce (ICC)
  http://www.iccwbo.org/index.asp
- Internet Law Policy Forum (ILPF)
  http://www.ilpf.org/

- *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, The Internet Engineering Task Force, March 1999
  ftp://ftp.isi.edu/in-notes/rfc2527.txt
- *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, OECD, October 1999
  http://www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final
- *Issues Relating to the Use of Electronic Authentication*, Electronic Authentication Task Group, APEC Telecommunications Working Group
  http://www.apii.or.kr/telwg/eaTG/eaTG-2.htm

  Annexes:
  http://www.apii.or.kr/telwg/eaTG/eaTG-cont.html

- Joint OECD-Private Sector Workshop on Electronic Authentication, June 1999.
  http://www.oecd.org/dsti/sti/it/index.htm
- PKI (Public-Key Infrastructure) Forum
  http://www.pkiforum.org/
- *Ministerial Declaration on Authentication for Electronic Commerce*, OECD, October 1998
  http://appli1.oecd.org/OLIS/1998DOC.NSF/fa23c92092a26efac12560b60038aa17/90270c904b319965c12566dd003230fd/$FILE/12E89552.ENG
- *The Global Action Plan for Electronic Commerce*, Alliance for Global Business (AGB), Global Information Infrastructure Commission (GIIC)
  http://www.gii.org/focus/ecommerce/agbecplan.html